

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claim 1 has been amended to incorporate the elements of claim 35. Claim 2 has been amended to incorporate the elements of claim 36. Claims 9-36 are canceled without prejudice. Claims 1-8 are pending in this application.

35 U.S.C. § 103

Claims 1-3, 8-11, 14-16, 18-20, 22-24, 31, and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,530,752 to Rubin (hereinafter "Rubin") in view of U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida") and further in view of U.S. Patent No. 6,473,860 to Chan (hereinafter "Chan"). Claims 9-11, 14-16, 18-20, 22-24, 31, and 33 are canceled without prejudice, thereby rendering the rejection of claims 9-11, 14-16, 18-20, 22-24, 31, and 33 moot. Applicant respectfully submits that claims 1-3 and 8 are allowable over Rubin in view of Yoshida and further in view of Chan.

With respect to claim 1, claim 1 recites:

An installation module comprising:
an encrypted software module that is a first version of the software module;
a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm; and
an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system and to install the first version of the software module on the computing system when at least one of the set of trigger files is stored on the computing system, wherein each

of the trigger files indicates authorization to install the encrypted software module, and wherein the first version of the software module uses greater than a threshold strength encryption;

wherein a second version of the software module is installed if at least one of the set of trigger files is not stored on the computing system, and wherein the second version of the software module uses a strength encryption that is not greater than the threshold strength encryption.

Claim 1 has been amended to incorporate the elements of its dependent claim 35. In the July 1, 2005 Office Action, claim 35 was rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin in view of Yoshida and further in view of Chan and U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis") and further in view of U.S. Patent No. 6,192,474 to Patel (hereinafter "Patel '474").

In the July 1, 2005 Office Action at p. 8, Patel '474 at col. 2, lines 37-59 is cited as disclosing using a hash of authentication information as an encryption key. The cited portion of Patel '474 discusses calculating a value $(g^{R_M R_N} \bmod p)$ as part of a Diffie-Hellman Encrypted Key Exchange and using a hash thereof as a session key (see, col. 2, lines 56-69). However, in the July 1, 2005 Office Action at pp. 4-5, the decryption key 305 of Rubin is relied on as disclosing the decryption key of claim 1 while the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 1 (see, July 1, 2005 Office Action at pp. 4-5). Thus, in order to satisfy the language of claim 1, there would need to be some disclosure or suggestion to encrypt the decryption key 305 of Rubin as a function of a cryptographic hash value produced by hashing the version number of Rubin. Applicant respectfully submits that the mere discussion of using a hash of a value calculated as part of a Diffie-Hellman Encrypted Key Exchange as a session key in Patel '474 does not provide any disclosure or suggestion of hashing the version

number of Rubin, much less of using the resulting cryptograph hash value to encrypt a decryption key. There is no discussion or mention in Rubin or Patel '474 to use a value derived from a trigger file to encrypt a decryption key, much less of the decryption key being encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. Without any such discussion or mention, Applicant respectfully submits that Rubin and Patel '474 cannot disclose or suggest a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

Furthermore, in the July 1, 2005 Office Action at p. 3, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hash value as an encryption key in Davis in order to add security prior to establishing the key as taught in Patel (Col. 3, lines 36-38). However, there still is no assertion that a hash value is produced by hashing a corresponding trigger file as recited in claim 1. As the version number from the Executable Object Code System Program of Rubin is relied on as disclosing the at least one of a set of trigger files of claim 1, Applicant respectfully submits that in order to disclose the elements of claim 1 there must be some disclosure or suggestion that the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. As there is no discussion or mention of hashing the version number of Rubin or of why one would want to hash the version number of Rubin, much less of using the hashed version number or of why one would want to use the hashed version number for

encrypting the decryption key, Applicant respectfully submits that Rubin in view of Patel '474 cannot disclose or suggest wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

Yoshida, Chan, and Davis are not cited as curing, and do not cure, these deficiencies of Rubin in view of Patel '474.

In addition, in the July 1, 2005 Office Action at p. 3, it was asserted that it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64). As discussed above, however, in order to disclose the elements of claim 1 there must be some disclosure or suggestion that the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm. Applicant respectfully submits that a hash of a version number does not authenticate any sender of information, and thus that there is no suggestion that the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a version number with a hash algorithm in the cited references. Accordingly, for at least these reasons, Applicant respectfully submits that the cited references do not disclose or suggest a decryption key to decrypt the encrypted software module, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 1.

Accordingly, Applicant respectfully submits that claim 1 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474.

With respect to claim 2, claim 2 has been amended to incorporate the elements of its dependent claim 36. Applicant respectfully submits that, similar to the discussion above regarding claim 1, Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474 does not disclose or suggest an installation module comprising a key, wherein the key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in claim 2. Accordingly, Applicant respectfully submits that claim 2 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Patel '474.

With respect to claim 3, given that claim 3 depends from claim 2, Applicant respectfully submits that claim 3 is allowable over Rubin in view of Yoshida and further in view of Chan for at least the reasons discussed above with respect to claim 2.

With respect to claim 8, given that claim 8 depends from claim 1, Applicant respectfully submits that claim 8 is allowable over Rubin in view of Yoshida and further in view of Chan for at least the reasons discussed above with respect to claim 1.

Claims 4, 6, 12, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin in view of Yoshida and further in view of Chan and further in view of U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis").

Claims 12 and 21 are canceled without prejudice, thereby rendering the rejection of claims 12 and 21 moot. Applicant respectfully submits that claims 4 and 6 are allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis.

Claims 4 and 6 depend from independent claims 2 and 1, respectively. Applicant respectfully submits that claims 4 and 6 are allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis for at least the reasons discussed above with respect to claims 2 and 1, respectively.

Claims 7 and 13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of U.S. Patent No. 5,825,890 to Elgamal et al. (hereinafter "Elgamal"). Claim 13 is canceled without prejudice, thereby rendering the rejection of claim 13 moot. Applicant respectfully submits that claim 7 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Elgamal.

Claim 7 depends from claim 6. Applicant respectfully submits that claim 7 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis due to its dependency on claim 6. Elgamal is not cited as curing, and does not cure, the deficiencies of Rubin in view of Yoshida and further in view of Chan and further in view of Davis discussed above with respect to claim 6. For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Rubin in view of Yoshida and further in view of Chan and further in view of Davis and further in view of Elgamal.

claims are allowable over the cited references for at least the reasons discussed above regarding claims 1 and 2.

Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-8 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 11/4/05

By: 

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256